



Supplementary terms for the supply of Managed Security Services

The Services set out in these Supplementary Terms shall be supplied by Apex Computing to the Customer on the terms and conditions set out in Apex Computing's General Terms and Conditions and those of these Supplementary Terms.

1. SUPPLEMENTARY DEFINITIONS

- 1.1 'Cloud-Based Utilities' means the collection of ancillary third-party provided services, including backup, anti-Malware, and monitoring services which will be used by Apex Computing in support of the Managed Security Services.
- 1.2 'Configuration' means the configuration of the IT Equipment, Hosted Services or component thereof, including hardware, installed software and all associated settings and / or parameters.
- 1.3 'Data Centre' means a remote data storage facility.
- 1.4 'Data Security Event' means a breach of the security of the Customer's infrastructure resulting in loss or damage, including loss of user-names, passwords, Personal Data; crypto-locking or other Malware-related damage.
- 1.5 'Device' means an item of IT Equipment including servers, workstations, laptop computers, tablets, mobile telephones, routers and firewalls.
- 1.6 'Emergency Maintenance' means any period of maintenance for which, due to reasons beyond its reasonable control, Apex Computing is unable to provide prior notice of.
- 1.7 'End User' means a user of the IT Equipment.
- 1.8 'Hosted Services' means Software that is hosted in a Microsoft 365 tenant and accessed by the Customer remotely.
- 1.9 'Hours of Cover' means the times that the Service Desk is available to respond to Incidents, and is set out in the Service Schedule.
- 1.10 'IT Equipment' means the Devices to be covered under the terms of this Agreement including those listed on the Order and any Devices subsequently discovered by Apex Computing's Monitoring Services.
- 1.11 'Managed IT Services' means the IT support services that may be provided by Apex Computing under the terms of an agreement for the supply of such.
- 1.12 'Managed Security Services' means the Managed Security Services described in the Service Schedule.
- 1.13 'Monitoring Agent' means Software which is installed on the IT Equipment and / or Hosted Services by Apex Computing which enables security monitoring and reporting.
- 1.14 'Monitoring Services' means Apex Computing's services which enable the delivery of the Managed Security Services.
- 1.15 'Penetration Test' means an automatic or manual check of the Customer's systems configuration pertaining to cyber security which is performed by Apex Computing.
- 1.16 'Security Issue' means an observed discrepancy which may be Security Threat.
- 1.17 'Security Threat' means a Security Issue that has been triaged and determined to be a threat to the integrity of the Hosted Services.
- 1.18 'Security Update' means security updates provided by third-party software and hardware vendors.
- 1.19 'Service Desk' means Apex Computing's dedicated team of qualified support specialists.

- 1.20 'Site' means Customer's site(s) at which IT Equipment is located, as set out in the Order.
- 1.21 'Software' means the software which is installed on the IT Equipment and / or Hosted Services by Apex Computing to enable the Managed Security Services.
- 1.22 'Subscription' means a subscription to subscription-based services.

2. TERM

- 2.1 This Agreement will be deemed to come into effect on the Commencement Date and shall run until the RFS Date (the 'Run-Up Period') and following the RFS Date for the Minimum Term as set out in the Order.

This Agreement shall continue to run after the expiry of the Minimum Term (or subsequent Additional Term) for an Additional Term. Apex Computing shall, not less than twenty-eight days prior to the end of the Minimum Term or any Additional Term thereafter, notify the Customer of changes to Charges and any other changes to the terms of this Agreement. In the event that:

- 2.1.1 The Customer serves notice to terminate this Agreement in accordance with clause 11 of the General Terms and Conditions or clause 9 hereof, this Agreement shall terminate at the end of the Minimum Term or Additional Term thereafter;
- 2.1.2 The Customer notifies Apex Computing of acceptance of changes, the Agreement shall continue in force for an Additional Term;

The Customer fails to notify Apex Computing of acceptance of changes and fails to serve notice to terminate, such failures to notify Apex Computing shall imply that the changes have been accepted and the Agreement shall continue in force for an Additional Term.

- 2.2 The duration of any Additional Term shall be the same as the Minimum Term, unless otherwise set out on the Order.

3. PROVISION OF SERVICES

- 3.1 Managed Security Services are provided to merely mitigate the cyber vulnerability of the IT Equipment and / or Hosted Services.
- 3.2 The Service Components to be provided under the terms of this Agreement are described in the Service Schedule.
- 3.3 Managed Security Services will be provided by Apex Computing remotely.
- 3.4 The Managed Security Services do not include the provision of a Service Desk:
 - 3.4.1 If Apex Computing provides Managed IT Services to the Customer under a separate agreement, Apex Computing will provide Service Desk support for the Managed Security Services to the Customer under the terms of the agreement for the supply of Managed IT Services;

If Apex Computing does not provide Managed IT Services to the Customer under a separate agreement, Apex Computing will provide Service Desk support for the Managed Security Services to the Customer on a chargeable basis, as set out in sub-clause 10.3.

- 3.5 For the avoidance of doubt, Managed Security Services do not include IT systems support, hardware maintenance or local area network support.
- 3.6 During the term of this Agreement, Apex Computing shall be entitled to make alterations to the Configuration of the IT Equipment and / or Hosted Services. Such alterations may result in temporary disruption to the availability of the IT Equipment and / or Hosted Services and Apex Computing will use reasonable endeavours to minimise such disruption and will provide as much notice as possible prior to such disruption.
- 3.7 Apex Computing cannot guarantee and does not warrant that the Managed Security Services shall result in the IT Equipment and / or Hosted Services operating free from interruptions or will be free from the risk of Malware infection or other Data Security Event.

- 3.8 A number of the Managed Security Services include Monitoring Services; and
- 3.8.1 Apex Computing shall use reasonable endeavours to provide the Monitoring Services 24 x 7 x 365;
- 3.8.2 Apex Computing cannot guarantee and does not warrant that the Monitoring Services will be free from interruptions, including:
- a) Interruption of the Monitoring Services for operational reasons and temporary degradation of the quality of the Monitoring Services;
 - b) Interruption of the connection of the Monitoring Services to other network services provided either by Apex Computing or a third party; and
 - c) Any such interruption of the Monitoring Services referred to in this sub-clause shall not constitute a breach of this Agreement.

4. ACCEPTABLE USE

- 4.1 The Customer agrees to use the IT Equipment and / or Hosted Services in accordance with the provisions of this Agreement, any relevant service literature and all other reasonable instructions issued by Apex Computing from time to time.
- 4.2 The Customer agrees to ensure that the IT Equipment and / or Hosted Services is not used by its End Users to:
- 4.2.1 Post, download, upload or otherwise transmit materials or data which is abusive, defamatory, obscene, indecent, menacing or disruptive;
 - 4.2.2 Post, download, upload or otherwise transmit materials or data uploads or make other communications in breach of the rights of third parties, including but not limited to those of quiet enjoyment, privacy and copyright;
 - 4.2.3 Carry out any fraudulent, criminal or otherwise illegal activity;
 - 4.2.4 In any manner which in Apex Computing's reasonable opinion brings Apex Computing's name into disrepute;
 - 4.2.5 Knowingly make available or upload files that contain Malware or otherwise corrupt data;
 - 4.2.6 Falsify true ownership of software or data contained in a file that the Customer or End User makes available via IT Equipment and / or Hosted Services;
 - 4.2.7 Falsify user information or forge addresses;
 - 4.2.8 Act in any way which threatens the security or integrity of the IT Equipment, Hosted Services or Cloud-Based Utilities, including the download, intentionally or negligently, of Malware;
 - 4.2.9 Violate general standards of internet use, including denial of service attacks, web page defacement and port or number scanning;
 - 4.2.10 Connect to the IT Equipment and / or Hosted Services insecure equipment or services able to be exploited by others to carry out actions which constitute a breach of this Agreement including the transmission of unsolicited bulk mail or email containing infected attachments or attempts to disrupt websites and/or connectivity or any other attempts to compromise the security of other users of Apex Computing's network or any other third-party system;
- 4.3 The Customer acknowledges that it is responsible for all data and/or traffic originating from the IT Equipment and / or Hosted Services.
- 4.4 The Customer agrees to not and ensure that its End Users do not share passwords provided for access to Cloud-Based Utilities.

The Customer agrees, subject to the provisions of the General Terms and Conditions to indemnify Apex Computing against all costs, damages, expenses or other liabilities arising from any third-party claim which arises from the Customer's breach of this clause 4.

5. CUSTOMER'S OBLIGATIONS

- 5.1 During the term of this Agreement, the Customer shall:
- 5.2 Pay all agreed additional Charges levied by Apex Computing.
- 5.3 Ensure that user-names, passwords and personal identification numbers are kept secure.
- 5.4 Accept that it is the Customer's sole responsibility to take all reasonable steps to prevent the introduction of Malware into the IT Equipment and / or Hosted Services.
- 5.5 Be solely responsible for ensuring compliance with the terms of licence of any Software that is a component of the IT Equipment and / or Hosted Services that has been provided by the Customer.
- 5.6 Be responsible for providing external network connectivity, including access to the Public Internet, as required for the correct functioning of the Managed Security Services.
- 5.7 Be responsible for implementing (or requesting that Apex Computing implements) Apex Computing's recommendations and acknowledges if that such recommendations are not implemented, it may be impossible for Apex Computing to provide the Service, and failure to implement Apex Computing's recommendations will be deemed a material breach of this Agreement.

6. APEX COMPUTING'S OBLIGATIONS

During the term of this Agreement, and subject to the performance by the Customer of its obligations hereunder, Apex Computing shall:

- 6.1 Provide the Managed Security Services set out in the Order and described in the attached Service Schedule, subject to any service limitations set out on the Order and herein.

During the Hours of Cover and subject to the provisions of sub-clause 10.3, make available a Service Desk that shall provide support and guidance in the use of the Services and manage the resolution of any Incidents that arise in the Managed Security Services.

- 6.2 Be responsible for the licensing and installation of Monitoring Agents and all Software that Apex Computing installs on the IT Equipment and / or Hosted Services.
- 6.3 Register and maintain the Customer's Subscriptions to the third-party Hosted Services set out in this Agreement, subject to any service limitations set out in the Order and Service Schedule.

7. Clause Intentionally Unused

8. GENERAL

- 8.1 The installation of Security Updates may limit the availability of the IT Equipment and / or Hosted Services. Apex Computing will use reasonable endeavours to schedule Security Updates to minimise disruption to the Customer; and
 - 8.1.1 The Customer shall test its IT Equipment and / or Hosted Services once the Security Update has been applied to ensure it has not impacted their functionality. If a Security Update has an adverse effect on the operation of the Software, Apex Computing will where possible remove the Security Update, in agreement with the Customer;
- 8.2 Apex Computing may be unable to provide prior notice of Emergency Maintenance to the Hosted Services, but will endeavour to minimise the impact of any such maintenance on the Customer.
- 8.3 If Apex Computing carries out work in response to an Incident reported by the Customer and Apex Computing subsequently determines that such Incident was not in the Managed Security Services or caused by any act or omission by Apex Computing, it shall be entitled to charge the Customer at its prevailing rate.
- 8.4 In the event of persistent breach of clause 4.2.8, Apex Computing shall be entitled to:
 - 8.4.1 Charge the Customer at its prevailing rate for the removal of Malware;
 - 8.4.2 Terminate this Agreement.

- 8.5 If the Customer suffers a Data Security Event and subsequently requests assistance from Apex Computing, it is the Customer's sole responsibility to ensure that such request for assistance will not breach the terms of any cyber-insurance policy that the Customer has in place, prior to requesting assistance from Apex Computing.
- 8.6 If the Customer is contacted by Apex Computing and requested to make a change to the Configuration of the IT Equipment and / or Hosted Services, it is the Customer's sole responsibility to verify the identity of the requestor prior to carrying out the requested change.
- 8.7 The Customer is responsible for the licensing of all other software, including Windows operating systems, Microsoft Office and line of business applications which have not been supplied by Apex Computing under the terms of any other agreement between Apex Computing and the Customer.
- 8.8 The Customer agrees not to reverse any security policy changes made by Apex Computing without the prior written consent of Apex Computing (such consent not to be unreasonably withheld or delayed).
- 8.9 The Customer hereby consents to Apex Computing and its sub-contractors and suppliers accessing the IT Equipment and Hosted Services, for the sole purpose of providing the Services; and
 - 8.9.1 Acknowledges that during the configuration of certain Service Components, Apex Computing, its sub-contractors and suppliers may require global administrative access to the Hosted Services.

9. TERMINATION

In addition to the provisions of clause 11 of the General Terms and Conditions, this Agreement may also be terminated:

By either party by giving the other not less than ninety days' notice in writing to terminate at the end of the Minimum Term or any Additional Term thereafter;

- 9.1.1 By Apex Computing at any time if it can no longer provide the Services;

- 9.1.2 By the Customer by reason of Apex Computing's un-remedied or repeated material breach of the terms of this Agreement;

By the Customer if Apex Computing or its supplier makes changes to the Managed IT Services which materially adversely affect the Customer (which for the avoidance of doubt, does not include changes to Charges).

10. CHARGES AND PAYMENT

- 10.1 Invoices for Recurring Charges shall be raised in advance of the relevant period. The invoicing period is set out in the Order.
- 10.2 Invoices for additional services, including any usage-based Charges, set-up and installation Charges will be raised in arrears.
- 10.3 Customers who use the Service Desk but do not have in place an agreement for the supply of Managed IT Services will be charged at Apex Computing's hourly rate with a minimum Charge for one hour per Incident.
- 10.4 Apex Computing shall commence charging for the Managed Security Services from the RFS Date, regardless of the date on which the Customer commences use of the Managed Security Services. If the RFS Date does not correspond with Apex Computing's invoicing period as set out in the Order, Apex Computing shall charge the Customer at a pro-rata rate for the first invoicing period.
- 10.5 The Customer acknowledges that the Charges for the Minimum Term are calculated by Apex Computing in consideration inter alia of the setup costs to be incurred by Apex Computing and the length of the Minimum Term offered.
- 10.6 The Customer agrees that it shall be liable for Early Termination Charges if this Agreement is terminated by:

- 10.6.1 The Customer terminating this Agreement for convenience prior to the end of the Minimum Term or Additional Term, whereupon the Customer shall be liable for the Recurring Charges payable for the remainder of the current term;
- 10.6.2 Apex Computing terminating this Agreement prior to the end of the Minimum Term or Additional Term by reason of the Customer's un-remedied breach of the terms of this Agreement, whereupon the Customer shall be liable for the Recurring Charges payable for the remainder of the current term.
- 10.7 The Customer shall not be liable for termination Charges if this Agreement is terminated by:
 - 10.7.1 The Customer at the end of the Minimum Term or any Additional Term thereafter PROVIDED THAT the Customer properly serves written notice to terminate, in accordance with clause 9 hereof;
 - 10.7.2 Apex Computing at any time if it can no longer provide the Services or part thereof;
 - 10.7.3 The Customer by reason of Apex Computing's un-remedied or repeated breach of the terms of this Agreement;
 - 10.7.4 A right of termination arises under the provisions of sub-clauses 9.1.2 to 9.1.5.

11. LIMITATIONS AND EXCLUSIONS

The following are not included under the terms of this Agreement:

- 11.1.1 IT policy and template design;
- 11.1.2 Compliance issues;
- 11.1.3 IT Equipment or Hosted Services support or maintenance;
- 11.1.4 Changes to the Configuration of the IT Equipment and / or Hosted Services other than those covered by the Managed Security Services;

On-Site support; Remediation, Malware removal or data restoration following a Malware attack.

Cyber questionnaires either insurance or supplier related

- 11.2 Apex Computing, if requested, may provide any of the excluded services listed above, and will charge for so doing at its prevailing rate.

12. EXCLUSION OF LIABILITY

- 12.1 The Customer acknowledges and agrees that:
 - 12.1.1 Any recommendations or advice provided by Apex Computing is intended to merely mitigate the Customer's cyber vulnerability and is provided without any warranty that that on implementing such recommendations or advice, the Customer will be free from cyber security vulnerabilities or their attendant risks;
 - 12.1.2 Apex Computing shall not be liable for any liabilities, losses, damages, costs, fines or expenses that result directly or indirectly from recommendations or advice provided by Apex Computing unless such recommendation or advice was either given negligently or was negligently withheld.
- 12.2 The Customer agrees that Apex Computing shall not be liable for any actions, losses damages, judgements, legal fees, costs, fines, claims or expenses incurred by the Customer or legal proceedings which are brought or threatened against the Customer by a third party in the event of:
 - 12.2.1 Any breaches by the Customer of any Data Protection Legislation;
 - 12.2.2 Any security breach of or vulnerability in the Customer's systems and processes.
- 12.3 All Managed Security Services are provided on an 'as is' basis, without warranty, guarantee of fitness for purpose or suitability for the Customer's purpose; and

12.3.1 Apex Computing shall not be liable for any damages or costs arising from a failure of any component of the Managed Security Services, including failure to detect Malware, Data Security Events or the requirement for Security Updates unless such failure is caused by the negligence of Apex Computing.

12.4 Apex Computing shall not be liable for any damages, costs or charges arising from damage to, or theft of backup data that is transmitted from the Customer's Site to the Data Centre via the Public Internet, nor for any other losses that occur due to reasons beyond its reasonable control.

Security Updates are supplied by Apex Computing-authorized software vendors and not Apex Computing. Apex Computing will use reasonable endeavours to prevent a Security Update causing an adverse reaction with any particular IT Equipment and / or Hosted Services configuration, but Apex Computing shall not be liable for any disruption resulting from the installation of Security Updates. In such circumstances, Apex Computing's sole responsibility will be to de-install the Security Update or roll back to an appropriate restore point to resolve the issue.

12.5 The Customer acknowledges and agrees that:

There is a small risk that Penetration Tests carried out by Apex Computing may cause problems in the Customer's IT systems, including routers and / or firewalls ceasing to function correctly and database and storage access issues;

12.5.1 The testing of the Customer's IT systems for correct functioning after Apex Computing's Penetration Tests and any necessary reconfiguration, and any associated costs shall be the Customer's sole responsibility;

Whilst Apex Computing warrants that it shall use reasonable care during the execution of Penetration Tests, Apex Computing shall not be liable for any losses or damage which arise either directly or indirectly from its access to the Customer's IT infrastructure.

12.6 The provisions of this clause 12 shall survive the termination of this Agreement in perpetuity.

Service Schedule

This paragraph summarises all of the security Service Components that Apex Computing can provide. The individual Service Components to be provided to the Customer under the terms of this Agreement are set out on the Order

13. Service On-boarding

Apex Computing shall install Software that is required to deliver the Services, on the IT Equipment and / or Hosted Services.

Apex Computing will review and where necessary recommend or make appropriate changes to the IT Equipment's and / or Hosted Services' configurations to ensure that the Services included on the Order can be delivered effectively.

14. Service Desk

14.1 Apex Computing's Service Desk provides support and assistance in the use of the Managed Security Services under the terms of its agreement for the supply of Managed IT Services where such agreement is in place with the Customer.

14.2 If an agreement for the supply of Managed IT Services is not in place, Apex Computing will provide Service Desk support for the resolution of Incidents on a reasonable endeavours basis, chargeable as set out in sub-clause 10.3.

14.3 The Customer shall raise Incident reports by one of the following methods:

- Via Email: servicedesk@apexcomputing.co.uk
- By Telephone to Apex Computing's Service Desk: 0161 233 0099

14.4 The Service Desk is available from 9am to 5pm Monday to Friday, excluding bank and public holidays.

15. Complaint Handling

15.1 If dissatisfied with any Services-related matter, the Customer should make a complaint using the following escalation path. If the complaint remains unresolved, the Customer should escalate to the next level in the escalation path:

Escalation Level	Role	Contact Details
1	Service Desk	servedesk@apexcomputing.co.uk 0161 233 0099
2	Complaints	complaints@apexcomputing.co.uk 0161 233 0099

15.2 Formal complaints can be made by e-mail or telephone, and will be responded to within three Working Days.

16. Apex Cyber Security Sphere

Apex Cyber Security Sphere is a package of Managed Security Services that are delivered by Apex Computing that are designed to mitigate risk from Cyber Threats. The solutions and services included can be changed / removed / implemented at the discretion of Apex Computing Services.

Optional Services may be supplied in addition to or independent of Apex Cyber Security Sphere, as set out on the Order.